UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

JENNIE CORONA-CANTU, on behalf of herself and all others similarly situated, Plaintiff, v. **INGO MONEY, INC.** Defendant.	Case No. **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Jennie Corona-Cantu ("Plaintiff"), individually and on behalf of all similarly situated persons, allege the following against Ingo Money, Inc. ("Ingo Money" or "Defendant") based upon personal knowledge with respect to herself and on information and belief derived from, among other things, investigation by Plaintiff's counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiff brings this class action against Ingo Money for its failure to properly secure and safeguard Plaintiff's and other similarly situated Ingo Money

customers' names, Social Security numbers, financial account information, driver's license numbers, and addresses (the "Private Information") from hackers.

2. Ingo Money, based in Alpharetta, Georgia, is a deposit risk management analytics and underwriting company that serves financial customers nationwide.

3. On or about June 27, 2024, Ingo Money filed official notice of a hacking incident with the Attorney General of the State of Texas.

4. On or about June 25, 2024, Ingo Money also sent out data breach letters to individuals whose information was compromised as a result of the hacking incident.

5. Based on the Notice filed by the company, on November 3, 2023, Ingo Money detected unusual activity on some of its computer systems. In response, the company initiated an investigation. The Ingo Money investigation revealed that an unauthorized party had access to certain company files sometime in the weeks before (the "Data Breach"). Yet, Ingo Money waited seven (7) months to notify the public that they were at risk.

6. As a result of this delayed response, Plaintiff and "Class Members" (defined below) had no idea for seven (7) months that their Private Information had been compromised, and that they were, and continue to be, at significant risk of

identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

7. The Private Information compromised in the Data Breach included highly sensitive data that represents a gold mine for data thieves, including but not limited to, financial account information and Social Security numbers that Ingo Money collected and maintained.

8. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

9. There has been no assurance offered by Ingo Money that all personal data or copies of data have been recovered or destroyed, or that Defendant has adequately enhanced its data security practices sufficient to avoid a similar breach of its network in the future.

10. Therefore, Plaintiff and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering ascertainable losses

in the form of harm from identity theft and other fraudulent misuse of their Private Information, the loss of the benefit of their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

11. Plaintiff brings this class action lawsuit to address Ingo Money's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and its failure to provide timely and adequate notice to Plaintiff and Class Members of the types of information that were accessed, and that such information was subject to unauthorized access by cybercriminals.

12. The potential for improper disclosure and theft of Plaintiff's and Class Members' Private Information was a known risk to Ingo Money, and thus Ingo Money was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

13. Upon information and belief, Ingo Money and its employees failed to properly monitor and to properly implement security practices with regard to the computer network and systems that housed the Private Information. Had Ingo Money properly monitored its networks, it would have discovered the Breach sooner.

14. Plaintiff's and Class Members' identities are now at risk because of Ingo Money's negligent conduct as the Private Information that Ingo Money

collected and maintained is now in the hands of data thieves and other unauthorized third parties.

15. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

16. Accordingly, Plaintiff, on behalf of herself and the Class, assert claims for negligence, negligence *per se*, breach of implied contract, violation of the California Consumer Protection Act, unjust enrichment, breach of third-party beneficiary contract, and declaratory judgment that this Court deems just and proper.

II. PARTIES

17. Plaintiff Jennie Corona-Cantu is, and at all times mentioned herein was, an individual citizen of the State of California.

18. Defendant Ingo Money is a deposit risk management analytics and underwriting company incorporated in Georgia, with its principal place of business at 11545 Wills Road, Ste. 130, Alpharetta, Georgia, 30009.

III. JURISDICTION AND VENUE

19. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the

number of class members is over 100, many of whom have different citizenship from Ingo Money. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

20. This Court has jurisdiction over Ingo Money because Ingo Money operates in and/or is incorporated in this District.

21. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District and Ingo Money has harmed Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

A. Ingo Money's Business and Collection of Plaintiff's and Class Members' Private Information

22. Ingo Money is a deposit risk management analytics and underwriting company. Founded in 2001, Ingo Money serves thousands of clients and their customers, including Plaintiff and Class Members, across the United States. Ingo Money employs more than 200 people and generates approximately $83 million in annual revenue.

23. As a condition of receiving financial services, Ingo Money requires that its clients' customers entrust it with highly sensitive personal information. In the ordinary course of receiving service from Ingo Money, Plaintiff and Class Members were required to provide their Private Information to Defendant.

24. Ingo Money uses this information, *inter alia*, to analyze and improve their site, manage accounts and access to materials on site, and marketing services.

25. In its privacy policy, Ingo Money promises its customers that it will not share this Private Information with third parties:

> "We will not sell, lease or trade your personal information to third parties unless we have your permission."[1]

26. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Ingo Money assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure and exfiltration.

27. Plaintiff and Class Members relied on Ingo Money to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this information, which Defendant ultimately failed to do.

B. The Data Breach and Ingo Money's Inadequate Notice to Plaintiff and Class Members

28. According to Defendant's Notice, it learned of unauthorized access to its computer systems on November 23, 2023, with such unauthorized access having taken place the weeks prior.

29. Through the Data Breach, the unauthorized cybercriminal(s) accessed a cache of highly sensitive Private Information, including names, Social Security numbers, financial account information, driver's license numbers, and addresses.

[1] https://ingomoney.com/ingo-money-privacy-policy/ (last visited on July 8, 2024).

30. On or about June 25, 2024, roughly seven (7) months after Ingo Money learned that the Class's Private Information was first accessed by cybercriminals, Ingo Money finally began to notify customers that its investigation determined that their Private Information was involved.

31. Ingo Money delivered Data Breach Notification Letters to Plaintiff and Class Members, alerting them that their highly sensitive Private Information had been exposed in a "data security incident."

32. The notice letter then attached some pages entitled "Additional Resources" and "ADDITIONAL STEPS YOU MAY WISH TO TAKE," which listed generic steps that victims of data security incidents can take, such as getting a copy of a credit report or notifying law enforcement about suspicious financial account activity. Other than providing one year of crediting monitoring that Plaintiff and Class Members would have to affirmatively sign up for and a call center number that victims could contact "with any questions," Ingo Money offered no other substantive steps to help victims like Plaintiff and Class Members to protect themselves. On information and belief, Ingo Money sent a similar generic letter to all individuals affected by the Data Breach.

33. Ingo Money had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members to keep

Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

34. Plaintiff and Class Members provided their Private Information to Ingo Money with the reasonable expectation and mutual understanding that Ingo Money would comply with its obligations to keep such information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

35. Ingo Money's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

36. Ingo Money knew or should have known that its electronic records would be targeted by cybercriminals.

C. Ingo Money Failed to Comply with FTC Guidelines

37. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

38. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

39. The FTC further recommends that companies not maintain Personally Identifiable Information ("PII") longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

40. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to

confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

41. As evidenced by the Data Breach, Ingo Money failed to properly implement basic data security practices. Ingo Money's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

42. Ingo Money was at all times fully aware of its obligation to protect the Private Information of its customers yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

D. Ingo Money Failed to Comply with Industry Standards

43. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

44. Some industry best practices that should be implemented by businesses like Ingo Money include but are not limited to educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and

limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

45. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

46. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

47. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

E. Ingo Money Breached its Duty to Safeguard Plaintiff's and Class Members' Private Information

48. In addition to its obligations under federal and state laws, Ingo Money owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining,

retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Ingo Money owed a duty to Plaintiff and Class Members to provide reasonable security, including complying with industry standards and requirements, training for its staff, and ensuring that its computer systems, networks, and protocols adequately protected the Private Information of Class Members

49. Ingo Money breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Ingo Money's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect customers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to sufficiently train its employees regarding the proper handling of its customers Private Information;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

f. Failing to adhere to industry standards for cybersecurity as discussed above; and

g. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

50. Ingo Money negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

51. Had Ingo Money remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential Private Information.

52. Accordingly, Plaintiff's and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft. Plaintiff and Class Members also lost the benefit of the bargain they made with Ingo Money.

F. Ingo Money Should Have Known that Cybercriminals Target Private Information to Carry Out Fraud and Identity Theft

53. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiff and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[2] Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

54. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

[2] *FTC Information Injury Workshop, BE and BCP Staff Perspective*, Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited on July 8, 2024).

55. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

56. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

57. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class Members' Private Information to access accounts, including, but not limited to, email accounts

and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiff and Class Members.

58. One such example of this is the development of "Fullz" packages.

59. Cybercriminals can cross-reference two sources of the Private Information compromised in the Data Breach to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

60. The development of "Fullz" packages means that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card or financial account numbers may not be included in the Private Information stolen in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other Class Members' stolen Private Information are being misused, and that such misuse is fairly traceable to the Data Breach.

61. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[3] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

62. Identity thieves can also use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house in the victim's name, receive medical services in the victim's name, and even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

[3] *See IdentityTheft.gov*, Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited July 8, 2024).

63. PII is data that can be used to detect a specific individual. PII is a valuable property right. Its value is axiomatic, considering the value of big data in corporate America and the consequences of cyber thefts (which include heavy prison sentences). Even this obvious risk-to-reward analysis illustrates beyond doubt that PII has considerable market value.

64. The U.S. Attorney General stated in 2020 that consumers' sensitive personal information commonly stolen in data breaches "has economic value."[4] The increase in cyberattacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry.

65. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, PII can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[5] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark

[4] *See Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax*, U.S. Dep't of Justice, Feb. 10, 2020, available at https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-fourmembers-china-s-military (last visited on July 8, 2024).

[5] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited on July 8, 2024).

web and that the "*fullz*" (a term criminals who steal credit card information use to refer to a complete set of information on a fraud victim) sold for $30 in 2017.[6]

66. Furthermore, even information such as names, email addresses and phone numbers, can have value to a hacker. Beyond things like spamming customers, or launching phishing attacks using their names and emails, hackers, *inter alia*, can combine this information with other hacked data to build a more complete picture of an individual. It is often this type of piecing together of a puzzle that allows hackers to successfully carry out phishing attacks or social engineering attacks. This is reflected in recent reports, which warn that "[e]mail addresses are extremely valuable to threat actors who use them as part of their threat campaigns to compromise accounts and send phishing emails."[7]

67. The Dark Web Price Index of 2022, published by PrivacyAffairs[8] shows how valuable just email addresses alone can be, even when not associated with a financial account:

---

[6] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited on July 8, 2024).

[7] *See* https://www.magicspam.com/blog/dark-web-price-index-the-cost-of-email-data/ (last visited on July 8, 2024).

[8] *See* https://www.privacyaffairs.com/dark-web-price-index-2022/ (last visited on July 8, 2024).

Email Database Dumps	Avg. Price USD (2022)
10,000,000 USA email addresses	$120
600,000 New Zealand email addresses	$110
2,400,000 million Canada email addresses	$100

68. Beyond using email addresses for hacking, the sale of a batch of illegally obtained email addresses can lead to increased spam emails. If an email address is swamped with spam, that address may become cumbersome or impossible to use, making it less valuable to its owner.

69. Likewise, the value of PII is increasingly evident in our digital economy. Many companies including Ingo Money collect PII for purposes of data analytics and marketing. These companies, collect it to better target customers, and shares it with third parties for similar purposes.[9]

70. One author has noted: "Due, in part, to the use of PII in marketing decisions, commentators are conceptualizing PII as a commodity. Individual data points have concrete value, which can be traded on what is becoming a burgeoning market for PII."[10]

[9] *See* https://robinhood.com/us/en/support/articles/privacy-policy/ (last visited on July 8, 2024).

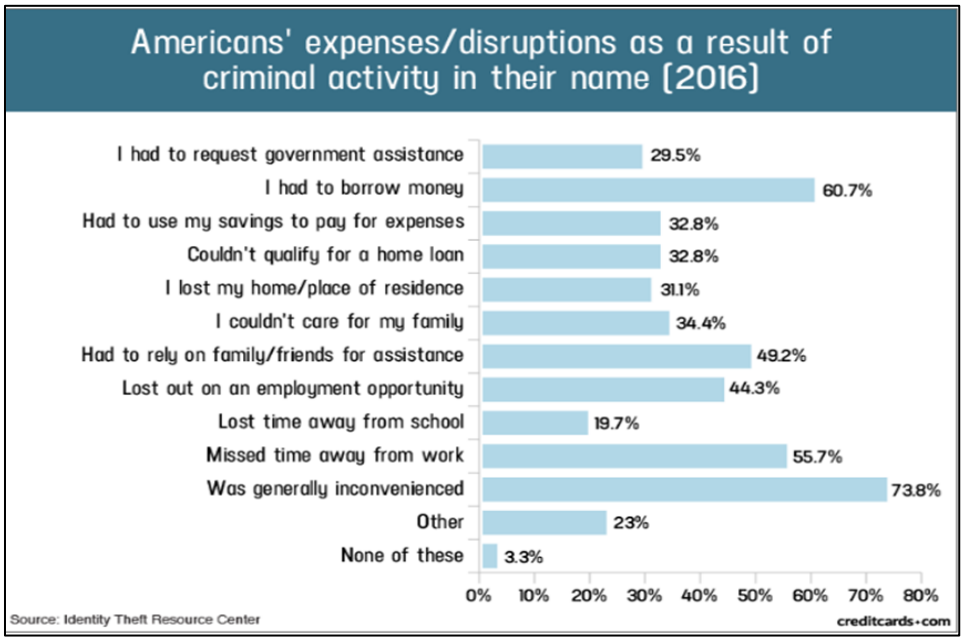
[10] *See* John T. Soma, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ('PII') Equals the "Value" of Financial Assets,* 15 Rich. J. L. & Tech. 11, 14 (2009).

71. Consumers also recognize the value of their personal information and offer it in exchange for goods and services. The value of PII can be derived not only by a price at which consumers or hackers actually seek to sell it, but rather by the economic benefit consumers derive from being able to use it and control the use of it.

72. A consumer's ability to use their PII is encumbered when their identity or credit profile is infected by misuse or fraud. For example, a consumer with false or conflicting information on their credit report may be denied credit. Also, a consumer may be unable to open an electronic account where their email address is already associated with another user. In this sense, among others, the theft of PII in the Data Breach led to a diminution in value of the PII.

73. Data breaches, like that at issue here, damage consumers by interfering with their fiscal autonomy. Any past and potential future misuse of Plaintiff's PII impairs their ability to participate in the economic marketplace.

74. A study by the Identity Theft Resource Center[11] shows the multitude of harms caused by fraudulent use of PII:



75. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or personal financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[12]

[11] Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), *available at* https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (last visited July 8, 2024).

[12] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/assets/270/262904.html (last visited July 8, 2024).

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

76. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

77. As a result, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

G. Plaintiff's and Class Members' Damages

Plaintiff Corona-Cantu's Experience

78. Plaintiff Corona-Cantu was a customer of one of Ingo Money's clients and, as such, Defendant came into possession and control of substantial amounts of her PII.

79. On or about June 25, 2024, Plaintiff Corona-Cantu received a letter entitled "Notice of Data Breach" which told her that the Private Information with which she had entrusted Defendant was impacted during the Data Breach. Specifically, the Notice informed her that the Private Information compromised included her "name, date of birth, and Social Security number."

80. The Notice offered her only one (1) year of credit monitoring services. This offer is insufficient given that Plaintiff Corona-Cantu will now experience a lifetime of increased risk of identity theft and other forms of targeted fraudulent misuse of her Private Information.

81. Plaintiff Corona-Cantu suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring her accounts for fraud.

82. Plaintiff Corona-Cantu would not have permitted that her Private Information be provided to Defendant had Defendant timely disclosed that its systems lacked adequate computer and data security practices to safeguard its clients' customers' personal information from theft, and that those systems were subject to a data breach.

83. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff suffered injury from a loss of privacy.

84. Plaintiff suffered actual injury in the form of having her Private Information compromised and stolen by cyber thieves in the Data Breach.

85. Plaintiff Corona-Cantu suffered actual injury in the form of damages to and diminution in the value of her personal and financial information – a form of intangible property that Plaintiff Corona-Cantu permitted to be entrusted to

Defendant for the purpose of receiving fintech services from Defendant's client(s) and which was compromised in, and as a result of, the Data Breach.

86. Plaintiff Corona-Cantu suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by her Private Information being placed in the hands of criminals.

87. Plaintiff Corona-Cantu has a continuing interest in ensuring that her Private Information, which remains in the possession of Defendant, is protected and safeguarded from future breaches.

88. As a result of the Data Breach, Plaintiff Corona-Cantu made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendant, as well as long-term credit monitoring options she will now need to use. Plaintiff has spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities.

89. As a result of the Data Breach, Plaintiff Corona-Cantu has suffered anxiety as a result of the release of her Private Information to cybercriminals, which Private Information she believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of committing cyber and

other crimes against her. Plaintiff is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach will have on her life.

90. Plaintiff Corona-Cantu also suffered actual injury as a result of the Data Breach in the form of (a) damage to and diminution in the value of her Private Information, a form of property that Defendant obtained from Plaintiff; (b) violation of her privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud she now faces.

91. As a result of the Data Breach, Plaintiff Corona-Cantu anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

92. In sum, Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

93. Plaintiff's Private Information was taken from Defendant as a direct and proximate result of the Data Breach, which Data Breach resulted from Defendant's inadequate data security practices.

94. As a direct and proximate result of Ingo Money's actions and omissions, Plaintiff and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, loans

opened in their names, tax returns filed in their names, utility bills opened in their names, credit card accounts opened in their names, and other forms of identity theft.

95. Further, as a direct and proximate result of Ingo Money's conduct, Plaintiff and Class Members have been forced to spend time dealing with the effects of the Data Breach.

96. Plaintiff and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiff and Class Members.

97. The Private Information maintained by and stolen from Defendant's systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiff and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiff and Class Members.

98. Additionally, as a direct and proximate result of Ingo Money's conduct, Plaintiff and Class Members have also been forced to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely

reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

99. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

100. Additionally, Plaintiff and Class Members also suffered a loss of value of their PII and PHI when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[13] In fact, consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to $50 a year.[14]

101. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to

[13] *See* https://thequantumrecord.com/blog/data-brokers-profit-from-our-data/#:~:text=The%20business%20of%20data%20brokering,annual%20revenue%20of%20%24200%20billion. (last visited on July 8, 2024).

[14] *Frequently Asked Questions,* Nielsen Computer & Mobile Panel, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited July 8, 2024).

Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiff and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiff and the Class Members, thereby causing additional loss of value.

102. Finally, Plaintiff and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach. These losses include, but are not limited to, the following:

a. Monitoring for and discovering fraudulent activity;
b. Addressing their inability to withdraw funds linked to compromised accounts;
c. Taking trips to banks and waiting in line to obtain funds held in limited accounts;
d. Spending time on the phone with or at a financial institution to dispute fraudulent charges;
e. Contacting financial institutions and closing or modifying financial accounts;

f. Closely reviewing and monitoring bank accounts and credit reports for additional unauthorized activity for years to come.

103. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of Ingo Money, is protected from future additional breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

104. As a direct and proximate result of Ingo Money's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

V. CLASS ACTION ALLEGATIONS

105. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

106. Specifically, Plaintiff proposes the following Nationwide Class, as well as the following California Subclass definition (also collectively referred to herein as the "Class"), subject to amendment as appropriate:

Nationwide Class

All individuals in the United States who had Private Information accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.

California Subclass

All residents of California who had Private Information accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.

107. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

108. Plaintiff reserves the right to modify or amend the definitions of the proposed Nationwide Class, as well as the California Subclass before the Court determines whether certification is appropriate.

109. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

110. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of thousands of customers of Ingo Money whose data was compromised in

the Data Breach. The identities of Class Members are ascertainable through Ingo Money's records, Class Members' records, publication notice, self-identification, and other means.

111. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Ingo Money engaged in the conduct alleged herein;

b. Whether Ingo Money's conduct violated the CCPA invoked below;

c. When Ingo Money learned of the Data Breach;

d. Whether Ingo Money's response to the Data Breach was adequate;

e. Whether Ingo Money unlawfully lost or disclosed Plaintiff's and Class Members' Private Information;

f. Whether Ingo Money failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

g. Whether Ingo Money's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

h. Whether Ingo Money's data security systems prior to and during the Data Breach were consistent with industry standards;

i. Whether Ingo Money owed a duty to Class Members to safeguard their Private Information;

j. Whether Ingo Money breached its duty to Class Members to safeguard their Private Information;

k. Whether hackers obtained Class Members' Private Information via the Data Breach;

l. Whether Ingo Money had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and the Class Members;

m. Whether Ingo Money breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

n. Whether Ingo Money knew or should have known that its data security systems and monitoring processes were deficient;

o. What damages Plaintiff and Class Members suffered as a result of Ingo Money's misconduct;

p. Whether Ingo Money's conduct was negligent;

q. Whether Ingo Money's conduct was *per se* negligent;

r. Whether Ingo Money was unjustly enriched;

s. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;

t. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

u. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

112. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach.

113. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

114. Predominance. Ingo Money has engaged in a common course of conduct toward Plaintiff and Class Members in that all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Ingo Money's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

115. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Ingo Money. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

116. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Ingo Money has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

117. Finally, all members of the proposed Class are readily ascertainable. Ingo Money has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Ingo Money.

VI. CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On behalf of Plaintiff and the Nationwide Class or Alternatively the California Subclass)

118. Plaintiff restates and realleges paragraphs 1-117 stated above as if fully set forth herein.

119. Ingo Money knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

120. Ingo Money's duty also included a responsibility to implement processes by which it could detect and analyze a breach of its security systems quickly and to give prompt notice to those affected in the case of a cyberattack.

121. Ingo Money knew or should have known of the risks inherent in collecting the Private Information of Plaintiff and Class Members and the importance of adequate security. Ingo Money was on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

122. Ingo Money owed a duty of care to Plaintiff and Class Members whose Private Information was entrusted to it. Ingo Money's duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. To protect its clients' customers' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiff and Class Members pursuant to the FTCA and CCPA;

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiff and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

123. Ingo Money's duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

124. Ingo Money's duty also arose because Defendant was bound by industry standards to protect its clients' customers' confidential Private Information.

125. Plaintiff and Class Members were foreseeable victims of any inadequate security practices on the part of Defendant, and Ingo Money owed them a duty of care to not subject them to an unreasonable risk of harm.

126. Ingo Money, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in

protecting and safeguarding Plaintiff's and Class Members' Private Information within Ingo Money's possession.

127. Ingo Money, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiff and Class Members.

128. Ingo Money, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

129. Ingo Money breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to comply with the FTCA;

f. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

130. Ingo Money acted with reckless disregard for the rights of Plaintiff and Class Members by failing to provide prompt and adequate individual notice of the Data Breach such that Plaintiff and Class Members could take measures to protect themselves from damages caused by the fraudulent use of the Private Information compromised in the Data Breach.

131. Ingo Money had a special relationship with Plaintiff and Class Members. Plaintiff's and Class Members' willingness to entrust Ingo Money with their Private Information was predicated on the understanding that Ingo Money would take adequate security precautions. Moreover, only Ingo Money had the ability to protect its systems (and the Private Information that it stored on them) from attack.

132. Ingo Money's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised and exfiltrated as alleged herein.

133. Ingo Money's breaches of duty also caused a substantial, imminent risk to Plaintiff and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

134. As a result of Ingo Money's negligence in breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

135. Ingo Money also had independent duties under state laws that required it to reasonably safeguard Plaintiff's and Class Members' Private Information and promptly notify them about the Data Breach.

136. As a direct and proximate result of Ingo Money's negligent conduct, Plaintiff and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

137. The injury and harm that Plaintiff and Class Members suffered was reasonably foreseeable.

138. Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

139. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring Ingo Money to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those

systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT II
NEGLIGENCE *PER SE*
(On behalf of Plaintiff and the Nationwide Class or Alternatively the California Subclass)

140. Plaintiff restates and realleges the allegations in paragraphs 1-117 as if fully set forth herein.

141. Pursuant to Section 5 of the FTCA, Ingo Money had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiff and Class Members.

142. Ingo Money breached its duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA, including but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

143. Plaintiff and Class Members are within the class of persons that the FTCA is intended to protect.

144. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect PII (such as the Private Information compromised in the Data Breach). The FTC rulings and publications described

above, together with the industry-standard cybersecurity measures set forth herein, form part of the basis of Ingo Money's duty in this regard.

145. Ingo Money violated the FTCA by failing to use reasonable measures to protect the Private Information of Plaintiff and the Class and by not complying with applicable industry standards, as described herein.

146. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiff's and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to Ingo Money's networks, databases, and computers that stored Plaintiff's and Class Members' unencrypted Private Information.

147. Ingo Money's violations of the FTCA constitute negligence *per se*.

148. Plaintiff's and Class Members' Private Information constitutes personal property that was stolen due to Ingo Money's negligence, resulting in harm, injury, and damages to Plaintiff and Class Members.

149. As a direct and proximate result of Ingo Money's negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to damages from the lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

150. Ingo Money breached its duties to Plaintiff and the Class under the FTCA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

151. As a direct and proximate result of Ingo Money's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

152. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring Ingo Money to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT III
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Nationwide Class or Alternatively the California Subclass)

153. Plaintiff restates and realleges the allegations in paragraphs 1-117 as if fully set forth herein.

154. Ingo Money provides deposit risk management analytics and underwriting services to its clients, which clients directly serve Plaintiff and Class Members. Plaintiff and Class Members, through their relationship with Defendant's clients, entrusted their Private Information to Defendant, thereby forming an implied

contract with Defendant regarding the provision of data security services sufficient to protect and safeguard such Private Information.

155. Defendant knew or should have known that it must protect Plaintiff's and Class Members' confidential Private Information in accordance with Ingo Money's policies, practices, and applicable law.

156. As consideration, Plaintiff and Class Members turned over valuable Private Information to Ingo Money. Accordingly, Plaintiff and Class Members bargained with Ingo Money to securely maintain and store such Private Information.

157. Ingo Money accepted possession of Plaintiff's and Class Members' Private Information for the purpose of providing services to Plaintiff and Class Members.

158. In delivering their Private Information to Ingo Money, Plaintiff and Class Members intended and understood that Ingo Money would adequately safeguard the Private Information.

159. Defendant's implied promises to Plaintiff and Class Members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the Private Information that is placed in the control of its employees is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees and/or agents; (4) designing and

implementing appropriate retention policies to protect the Private Information against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; and (7) taking other steps to protect against foreseeable data breaches.

160. Plaintiff and Class Members would not have permittedthat their Private Information be entrusted to Ingo Money in the absence of such an implied contract.

161. Had Ingo Money disclosed to Plaintiff and the Class that they did not have adequate computer systems and security practices to secure sensitive data, Plaintiff and Class Members would not have provided their Private Information to Ingo Money.

162. Ingo Money recognized that Plaintiff's and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain with Plaintiff and Class Members.

163. Ingo Money violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiff's and Class Members' Private Information.

164. Plaintiff and Class Members have been damaged by Ingo Money's conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

COUNT IV
VIOLATION OF CALIFORNIA CONSUMER PRIVACY ACT OF 2018
CAL. CIV. CODE §§ 1798.100 ET SEQ. ("CCPA")
(On behalf of Plaintiff and the California Subclass)

165. Plaintiff restates and realleges the allegations in paragraphs 1-117 as if fully set forth herein.

166. In 2018, the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. Among other things, the CCPA imposes an affirmative duty on certain businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected.

167. As fully alleged above, Defendants are subject to the CCPA and failed to implement these procedures or otherwise comply with the CCPA, which resulted in the Data Breach.

168. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure because of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

169. Plaintiff is a "consumer" as defined by Civ. Code § 1798.140(g) because she is natural person residing in the state of California.

170. Defendant is a "business" as defined by Civ. Code, § 1798.140(c).

171. The CCPA provides that "personal information" includes "[a]n individual's first name or first initial and the individual's last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted . . . (iii) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." *See* Civ. Code, § 1798.150(a)(1); Civ. Code, § 1798.81.5(d)(1)(A).

172. The information of Plaintiff's and the California Subclass constitutes "personal information" within the meaning of the CCPA.

173. The Data Breach occurred because of Defendants' failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, and as a result, Plaintiff's private information was unlawfully accessed.

174. Simultaneously herewith, Plaintiff is providing notice to Defendants pursuant to Civ. Code, § 1798.150(b)(1), identifying the specific provisions of the CCPA Plaintiff alleges Defendants have violated or are violating.

175. As a result, Plaintiff and the Class Members have been damaged in an amount to be proven at trial.

176. On behalf of herself and other members of the California Subclass, Plaintiff seeks statutory damages of up to $750 per class member, but no less than $100 per class member, actual damages to the extent they exceed statutory damages, injunctive and declaratory relief, and any other relief as deemed appropriate by the Court.

COUNT V
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Nationwide Class or Alternatively the California Subclass)

177. Plaintiff restates and realleges the allegations in paragraphs 1-117 as if fully set forth herein.

178. This Count is pleaded in the alternative to Count III above and Count VI below.

179. Plaintiff and Class Members conferred a benefit on Ingo Money by turning over their Private Information to Defendant and by paying for services that should have included cybersecurity protection to protect their Private Information. Plaintiff and Class Members did not receive such protection.

180. Upon information and belief, Ingo Money funds its data security measures entirely from its general revenue, including from payments made to it by

its clients, to which clients Plaintiff and Class Members provided their valuable Private Information.

181. As such, a portion of these payments is to be used to provide a reasonable and adequate level of data security that is in compliance with applicable state and federal regulations and industry standards, and the amount of the portion of each payment made that is allocated to data security is known to Ingo Money.

182. Ingo Money has retained the benefits of its unlawful conduct, including the amounts of payment received from its clients and the value of Plaintiffs' and Class Members' Private Information, which benefits should have been used for adequate cybersecurity practices that it failed to provide.

183. Ingo Money knew that Plaintiff and Class Members conferred a benefit upon it, which Ingo Money accepted. Ingo Money profited from these transactions and used the Private Information of Plaintiff and Class Members and the monies obtained therefrom for business purposes, while failing to use such benefits to fund adequate data security measures that would have secured Plaintiff's and Class Members' Private Information and prevented the Data Breach.

184. If Plaintiff and Class Members had known that Ingo Money had not adequately secured their Private Information, they would not have agreed to entrust their Private Information to Defendant.

185. Due to Ingo Money's conduct alleged herein, it would be unjust and inequitable under the circumstances for Ingo Money to be permitted to retain the benefit of its wrongful conduct.

186. As a direct and proximate result of Ingo Money's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) the loss of the opportunity to control how their Private Information is used; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Ingo Money's possession and is subject to further unauthorized disclosures so long as Ingo Money fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

187. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Ingo Money and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Ingo Money from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

188. Plaintiff and Class Members may not have an adequate remedy at law against Ingo Money, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT VI
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On behalf of Plaintiff and the Nationwide Class or Alternatively the California Subclass)

189. Plaintiff restates and realleges the allegations in paragraphs 1-117 as if fully set forth herein.

190. Defendant entered into contracts, written or implied, with its clients to perform services that include, but are not limited to, providing financial services. Upon information and belief, these contracts are virtually identical between and among Defendant and its clients around the country whose customers, including Plaintiff and Class Members, were affected by the Data Breach.

191. In exchange, Defendant agreed, in part, to implement adequate security measures to safeguard the Private Information of Plaintiff and the Class.

192. These contracts were made expressly for the benefit of Plaintiff and the Class, as Plaintiff and Class Members were the intended third-party beneficiaries of the contracts entered into between Defendant and its clients. Defendant knew that if it were to breach these contracts with its clients, the clients' customers Plaintiff and Class Members—would be harmed.

193. Defendant breached the contracts it entered into with its clients by, among other things, failing to (i) use reasonable data security measures, (ii) implement adequate protocols and employee training sufficient to protect Plaintiff's Private Information from unauthorized disclosure to third parties, and (iii) promptly and adequately detecting the Data Breach and notifying Plaintiff and Class Members thereof.

194. Plaintiff and the Class were harmed by Defendant's breach of its contracts with its clients, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result thereof.

195. Plaintiff and Class Members are also entitled to their costs and attorney's fees incurred in this action.

COUNT VII
DECLARATORY JUDGMENT
(On behalf of Plaintiff and the Nationwide Class or Alternatively the California Subclass)

196. Plaintiff restates and realleges the allegations in paragraphs 1-117 as if fully set forth herein.

197. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal and state statutes described in this Complaint.

198. Ingo Money owes a duty of care to Plaintiff and Class Members, which required it to adequately secure Plaintiff's and Class Members' Private Information.

199. Ingo Money still possesses Private Information regarding Plaintiff and Class Members.

200. Plaintiff alleges that Ingo Money's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of their Private Information and the risk remains that further compromises of their Private Information will occur in the future.

201. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Ingo Money owes a legal duty to secure its customers' Private Information and to timely notify customers of a data breach under the common law and Section 5 of the FTCA;

b. Ingo Money's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide

reasonable security procedures and practices that are appropriate to protect customers' Private Information; and

c. Ingo Money continues to breach this legal duty by failing to employ reasonable measures to secure customers' Private Information.

202. This Court should also issue corresponding prospective injunctive relief requiring Ingo Money to employ adequate security protocols consistent with legal and industry standards to protect customers' Private Information, including the following:

a. Order Ingo Money to provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, Ingo Money must implement and maintain reasonable security measures, including, but not limited to:

i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Ingo Money's systems on a periodic basis, and ordering Ingo Money to promptly correct any problems or issues detected by such third-party security auditors;

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Ingo Money's systems;

v. conducting regular database scanning and security checks;

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

vii. meaningfully educating its users about the threats they face with regard to the security of their Private Information, as well as the steps Ingo Money's customers should take to protect themselves.

203. If an injunction is not issued, Plaintiff will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at Ingo Money. The risk of another such breach is real, immediate, and substantial. If another breach

at Ingo Money occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

204. The hardship to Plaintiff if an injunction is not issued exceeds the hardship to Ingo Money if an injunction is issued. Plaintiff will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Ingo Money's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Ingo Money has a pre-existing legal obligation to employ such measures.

205. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at Ingo Money, thus preventing future injury to Plaintiff and other customers whose Private Information would be further compromised.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Classes described above, seek the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Nationwide Class and California Subclass requested herein;

b. Judgment in favor of Plaintiff and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing Ingo Money to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members;

e. An order requiring Ingo Money to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiff and Class Members awarding them reasonable attorneys' fees, costs, and expenses pursuant to O.C.G.A. Section 13-6-11 and as otherwise allowed by law;

g. A judgment in favor of Plaintiff and Class Members awarding them prejudgment and post-judgment interest; and

h. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

Respectfully submitted this 8th day of July, 2024.

/s/ MaryBeth V. Gibson
MaryBeth V. Gibson
GA Bar No. 725843
Gibson Consumer Law Group, LLC
4279 Roswell Road
Suite 208-108
Atlanta, GA 30342
Telephone: (678) 642-2503
marybeth@gibsonconsumerlawgroup.com

Tyler J. Bean *(pro hac vice forthcoming)*
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: tbean@sirillp.com

Counsel for Plaintiff and Putative Class

CERTIFCATE OF COMPLIANCE

I certify that the foregoing pleading has been prepared with Times New Roman, 14-point font, in compliance with L.R. 5.1B.

Dated: July 8, 2024.

/s/ MaryBeth V. Gibson
MaryBeth V. Gibson
GA Bar No. 725843
Gibson Consumer Law Group, LLC